

UNITED STATES DISTRICT COURT  
DISTRICT OF MINNESOTA

BRENDA CZECH, individually and on behalf of a class of similarly situated individuals,

Plaintiff,

V.

WALL STREET ON DEMAND, INC., a Delaware corporation, and JOHN DOES,

Defendants.

) File No.: No. 09-CV-180(DWF/RLE)

**PLAINTIFF’S MEMORANDUM  
OF LAW IN OPPOSITION TO  
DEFENDANT’S MOTION TO  
DISMISS**

## I. INTRODUCTION

Defendant Wall Street On Demand, Inc.’s (“WSOD”) *second* preliminary motion to short-circuit this class action at the pleading stage advances little new legal argument (it makes arguments it strategically chose not to raise until its reply brief on its initial motion for judgment on the pleadings) and once again asks this Court to dismiss this action at the pleading stage.

WSOD argues that plaintiff has not adequately stated claims under the Computer Fraud and Abuse Act ,18 U.S.C. §1030, *et seq.* (“CFAA”) because she has not adequately pled that WSOD acted “without authorization” when accessing her wireless device; that WSOD acted intentionally when doing so; that WSOD obtained information from plaintiff’s wireless device; and that WSOD caused damage to plaintiff’s wireless device. WSOD argues again that plaintiff has not adequately stated claims for trespass to chattels and unjust enrichment under state law, whichever state law that may be (WSOD does not

perform any choice-of-law analysis, so the Court is left to speculate which one should apply).

Although WSOD chides plaintiff for allegedly piling conclusions on top of conclusions, adding speculation to speculation, and neglecting allegations of fact in her second amended complaint, it is WSOD that uses the term “conclusion,” “conclusory,” or “speculation” no less than 35 times in its brief, in addition to citing to the Supreme Court’s recent *Twombly* or *Iqbal* decisions another eight times in support of its arguments. Repetition makes WSOD’s arguments no more compelling. Even though *Twombly* and *Iqbal* clarify the standard for evaluation of a motion to dismiss under Rule 12(b), they certainly do not “operate as a kind of universal ‘get out of jail free’ card.”<sup>1</sup>

Plaintiff, therefore, respectfully requests that this Court deny WSOD’s motion to dismiss and move this case into class and merits discovery.

## **II. ARGUMENT**

### **A. Standard of Review.**

In evaluating a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6), this Court should assume “all facts in the complaint to be true and construe[] all reasonable inferences from those facts in the light most favorable to the complainant.” *Czech v. Wall Street on Demand, Inc.*, No. 09-180, 2009 WL 2045308, \*1 (D. Minn. July 10, 2009) (citation omitted). “To survive a motion to dismiss, a complaint must contain ‘enough facts to state a claim to relief that is plausible on its face’” and must allege “‘enough fact[s] to raise a reasonable expectation that discovery will reveal evidence of

---

<sup>1</sup> Judge Milton I. Shadur, U.S.D.J., Northern District of Illinois (August 20, 2009).

[the claim].” *Id.* at \*2 (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 545, 546 (2007)). To state a claim under the CFAA, the standard is no different: “a plaintiff need only allege the required elements pursuant to Rule 8(a)(2)’s notice pleading standard, not the heightened pleading standard of Rule 9(b).” *Czech*, 2009 WL 2045308, at \*2 n.2 (citations omitted).

**B. Plaintiff Has Stated Claims Under The Computer Fraud And Abuse Act.**

**1. To State A Claim Under 28 U.S.C. § 1030(a)(2)(C) and 28 U.S.C. §§ 1030(a)(5)(A) and (a)(5)(C), Plaintiff Need Not Plead Both That WSOD “Obtained Information” And Caused “Damage” To Plaintiff’s Wireless Device.**

WSOD argues that, to state a claim under 28 U.S.C. § 1030(a)(2)(C) (2008),<sup>2</sup> plaintiff must allege, among other things, that “WSOD obtained information from Plaintiff’s cell phone, *and* WSOD caused damage to Plaintiff’s cell phone. Because Plaintiff has failed to allege the necessary factual predicate for . . . these required elements, her claim fails.” *See* WSOD Mem. at 5-6 (emphasis added). WSOD is as wrong as it is imprecise in its recitation of the required elements for plaintiff’s specific claim under Section 1030(a)(2)(C).

To plead a claim under Section 1030(a)(2)(C), which plaintiff has done in her second amended complaint at ¶¶ 90, 94-97, a plaintiff must allege, among other required elements, that a person “obtain[ed] information [from] any protected computer.” As the United States Court of Appeals for the Ninth Circuit recently observed, “CFAA prohibits

---

<sup>2</sup> As this Court did in its prior Order denying WSOD’s motion for judgment on the pleadings, plaintiff cites here to the 2008 version of CFAA, unless the context requires citation to a prior version of the statute. *See Czech*, 2009 WL 2045308, at \*2 n.1.

a number of different computer crimes, the majority of which involve accessing computers without authorization or in excess of authorization, and then taking specific forbidden actions, ranging from obtaining information to damaging a computer or computer data.” *LVRC Holdings LLC v. Brekka*, No. 07-17116, 2009 WL 2928952, \*3 (9th Cir. Sept. 15, 2009) (citation omitted) (emphasis added). There is no requirement under Section 1030(a)(2)(C) that a plaintiff also plead that the defendant caused “damage” to a protected computer in addition to “obtaining information” from that computer. *Id.*; see also *Paradigm Alliance, Inc. v. Celeritas Tech., LLC*, No. 07-1121, 2009 WL 3045464, \*18 (D. Kan. Sept. 22, 2009) (holding that Section 1030(a)(2)(C) does not require a plaintiff to show damage to a protected computer); *Czech*, 2009 WL 2045308, at \*3 (setting forth the elements of a claim under 28 U.S.C. § 1030(a)(2)(C) (2008)).

Similarly, to plead claims under 28 U.S.C. §§ 1030(a)(5)(A) and (a)(5)(C) (2008), which plaintiff also has alleged in her second amended complaint at ¶¶ 91-92, 98-102, a plaintiff must allege, among other required elements, that a person caused “damage” to a protected computer. See *Czech*, 2009 WL 2045308, at \*3 (setting forth the elements of a claim under 28 U.S.C. § 1030(a)(5)(A)). There is no requirement under Sections 1030(a)(5)(A) and (a)(5)(C) for a plaintiff to plead and show that the person also “obtained information” from a protected computer in addition to causing “damage” to the computer. *Id.*

**2. Plaintiff Has Alleged That WSOD Accessed Her Wireless Device “Without Authorization.”**

- a) The phrase “without authorization” in CFAA should be construed broadly and consistent with its ordinary and common meaning.**

WSOD contends plaintiff has not alleged that WSOD intentionally accessed her wireless device “without authorization” because there are only five ways a person can act “without authorization” under CFAA: (1) where an outside computer hacker “breaks into a computer”; (2) where a person accesses a protected computer in “violation of an agency or employment relationship”; (3) where a person accesses a protected computer in “violation of a contract”; (4) where a person accesses a protected computer in “violation of a rule or policy established by the owner that limits the scope of authorized access to the computer”; and (5) “by showing that the access exceeded the expected norms of intended use.” WSOD Mem. at 6-7 (citing cases).

To state a claim under Section 1030(a)(2)(C) (the section of CFAA relating to “obtaining information” from a protected computer), a person must intentionally access a protected computer “without authorization” and/or “exceed authorized access” to the protected computer. Although CFAA defines the phrase “exceed authorized access,” *see* 28 U.S.C. § 1030(e)(6) (2008), it does not define the term “without authorization.” *E.g., LVRC Holdings LLC*, 2009 WL 2928952, at \*4; *Vurv Tech. LLC v. Kenexa Corp.*, No. 08-3442, 2009 WL 2171042, \*6 (N.D. Ga. June 20, 2009) (same). Consequently, this Court should begin its statutory analysis with the plain language of CFAA, and should construe the phrase “without authorization” consistently with its “ordinary,

contemporary, common meaning.” *LVRC Holdings LLC*, 2009 WL 2928952, at \*4 (quoting *Perrin v. United States*, 444 U.S. 37, 42 (1979)); *see also United States v. Morris*, 928 F.2d 504, 511 (2d Cir. 1991) (same); *cf. Czech*, 2009 WL 2045308, at \*3 (holding “that a plain reading of the statute supports Czech’s interpretation” of 28 U.S.C. § 1030(c)(A)(i)(I) (2008)).

According to the Ninth Circuit, the “ordinary, contemporary, common meaning” of “authorization” is the “permission or power granted by an authority” and “the state of being authorized”; the meaning of “authorize” is “to endorse, empower, justify, permit by or as if by some recognized or proper authority.” *LVRC Holdings LLC*, 2009 WL 2928952, at \*4 (quoting *Random House Unabridged Dictionary* 139 (2001) and *Webster’s Third International Dictionary* 146 (2002)). As such, “a person who ‘intentionally accesses a protected computer without authorization’ . . . accesses a computer without any permission at all. . . .” *LVRC Holdings LLC*, 2009 WL 2928952, at \*5; *Condux Int’l, Inc. v. Haugum*, No. 08-4824, 2008 WL 5244818, \*4 (D. Minn. Dec. 15, 2008) (Montgomery, J.) (observing that the phrase “‘without authorization’ is not defined in the CFAA, but ‘authorization’ is commonly understood as ‘the act of conferring authority; permission’” (quotation and citation omitted)).<sup>3</sup>

---

<sup>3</sup> *See generally United States v. Drew*, --- F.R.D. ---, 2009 WL 2872855, \*11 (C.D. Cal. Aug. 28, 2009) (stating that “to ‘authorize’ ordinarily means ‘to give official approval to or permission for’ . . .” (quotation omitted); *U.S. Bioservices Corp. v. Lugo*, 595 F. Supp. 2d 1189, 1192 (D. Kan. 2009) (“[A]ccess to a protected computer occurs ‘without authorization’ only when initial access is not permitted, and a violation for ‘exceeding authorized access’ occurs only when initial access to the computer is permitted but the access of certain information is not permitted.”); *Vurv Tech. LLC*, 2009 WL 2171042, at \*6-7 (agreeing with the courts that have “held that a violation under the

Here, plaintiff alleges – and WSOD does not dispute in its motion – that she never gave WSOD her consent to send her any text messages. *E.g.*, 2d Am. Compl. at ¶¶ 64, 68, 95. Thus, under the plain language of CFAA, plaintiff has adequately pled that WSOD accessed her wireless device “without authorization” because she never gave WSOD permission to access her wireless device for any purpose, much less to send her unauthorized and unwanted text messages. *See LVRC Holdings LLC*, 2009 WL 2928952, at \*7 (holding “that a person uses a computer ‘without authorization’ . . . when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone’s computer without any permission)”; *cf. Satterfield v. Simon & Schuster, Inc.*, 569 F.3d 946, 954-55 (9th Cir. 2009) (interpreting the term “express consent” in the Telephone Consumer Protection Act and noting that “express consent” is commonly defined as “[c]onsent that is clearly and unmistakably stated” (quoting *Black’s Law Dictionary* 323 (8th ed. 2004))).

The cases cited by WSOD are inapposite. They apply (if at all) to circumstances where a person (usually a current or former employee) originally had *authorized* access to a protected computer. *See* WSOD. Mem. at 6-7 (citing cases). This is not such a case. *See Int’l Airports Centers, L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006) (former

---

CFAA for access ‘without authorization’ ‘occurs only where initial access is not permitted’” (citations omitted)); *Black & Decker (US), Inc. v. Smith*, 568 F. Supp. 2d 929, 935 (W.D. Tenn. 2008) (stating that “while there is no definition for access ‘without authorization,’ the Court finds that its plain meaning is ‘no access authorization.’” (citing *Lockheed Martin Corp. v. Speed*, No. 05-1580, 2006 WL 2683058, \*6 (M.D. Fla. Aug. 1, 2006)); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 963, 964-65 (D. Ariz. 2008) (citing cases and holding that “a violation of accessing a protected computer ‘without authorization’ occurs only when initial access is not permitted”).

employee acted “without authorization” because, before leaving his employ, he initially destroyed files in violation of the duty of loyalty that agency law imposes on an employee); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581-82 (1st Cir. 2001) (not deciding whether former employees’ access was “without authorization” but various former employees’ post-employment confidentiality agreements resulted in the former employees exceeding their authorized access to their former employer’s public website by subsequently using “scraper” software programs to mine data from the employer’s website); *United States v. Phillips*, 477 F.3d 215, 217, 220 (5th Cir. 2007) (college student violated an “acceptable use” computer policy through brute-force attacks that were “not an intended use of the [university computer] network within the understanding of any reasonable computer user”); *United States v. Morris*, 928 F.2d 504, 505, 510 (2d Cir. 1991) (college student was given “explicit authorization” to use the university’s computers but did not use the features of the computer system “in any way related to their intended function”).<sup>4</sup>

**b) Several CFAA cases have recognized that a person intentionally accesses a protected computer “without authorization” by sending bulk e-mail to the computer.**

As WSOD acknowledges, several CFAA cases have held (or at a minimum suggested) that a defendant intentionally accesses a protected computer “without authorization” or “exceeded authorized access” when sending bulk email to protected

---

<sup>4</sup> WSOD also cites *United States v. Mitra*, 405 F.3d 492, 493 (7th Cir. 2005). But the *Mitra* court does not cite, much less discuss, the scope of the phrase “without authorization.”

computers. *See Am. Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 450 (E.D. Va. 1998) (defendants acted “without authorization” when violating AOL’s terms of service); *cf. Am. Online, Inc. v. Nat’l Health Care Discount, Inc.*, 121 F. Supp. 2d 1255, 1273 (N.D. Iowa 2000) (denying motion for summary judgment where issue of whether defendants acted “without authorization” or “exceeded authorized access” required further factual development). Nonetheless, WSOD argues that these cases are distinguishable because “no ‘spam email’ case ever has upheld the application of the CFAA unless there has been a clear violation of a specific published rule prohibiting spam.” WSOD Mem. at 8.

Once again WSOD’s reasoning is fallacious because the fact that these courts have rested their conclusions on the fact that the conduct at issue violated a particular computer system’s (AOL’s) terms of service, does not necessarily mean that a violation of particular term or terms of service is the only way a person can act “without authorization” under CFAA. Simply put, none of the so-called “spam” e-mail cases created or even suggested a bright-line rule that a person acts “without authorization” only when he violates a “specific published rule” warning the person not to access a protected computer.

**c) Consumers such as plaintiff are not required to explicitly opt-out of receiving text messages to be protected by CFAA.**

Finally, WSOD claims that a consumer’s wireless device is the same as a publicly-accessible Internet website, and that CFAA “places the onus on the owner of the protected computer who wants to limit access to take affirmative action to do so and to

‘spell out’ for those seeking access ‘explicitly what is forbidden’ before permitting them access.” WSOD Mem. at 8 (citing *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 63 (1st Cir. 2003)). WSOD then invents and applies a “default rule” “that communication with a protected computer . . . is *with authorization* if such access is open to the public” and that plaintiff was required to communicate affirmatively a “rule or policy to WSOD that it was not authorized to send text messages to her” wireless device. *Id.* at 8-9 (citing *Citrin*, 440 F.3d at 420).

Leaving aside the impossibility of a wireless-device user expressly communicating or “spelling out” *ex ante* a “rule or policy” to the tens of thousands of potential senders of text messages that she does not wish to receive text messages from the senders, the cases WSOD cites undercut any argument it may have that a wireless-device user must affirmatively opt-out of receiving text messages to be protected by the CFAA because the cases acknowledge that lack of authorization may be implicit rather than explicit. *See EF Cultural Travel BV*, 318 F.3d at 63 (stating that, under certain circumstances, “lack of authorization may be implicit, rather than explicit” but that “the public website provider can easily spell out explicitly what is forbidden” when accessing the website) (emphasis added)). Moreover, as a matter of common sense a consumer’s wireless device should not be treated the same as a public Internet website, the latter of which is created specifically by its owner and operated to be accessed by the public (at least in a manner consistent with its proper or intended use).

Finally, WSOD’s made-up “default rule,” that commercial text-message communications with a wireless device are presumptively with authorization absent prior

notification by the wireless-device user to the sender that she does not wish to receive text messages, flies in the face of the federal government's current CAN-SPAM<sup>5</sup> regulations governing text messaging, which generally prohibit a person from sending unauthorized text messages to wireless devices using a text-message protocol that includes an e-mail address. *E.g.*, <http://www.fcc.gov/cgb/consumerfacts/canspam.html> ("The FCC's ban on sending unwanted e-mail messages to wireless devices applies to all 'commercial messages.' The CAN-SPAM Act defines commercial messages as those for which the primary purpose is to advertise or promote a commercial product or service.") (last visited October 9, 2009).

**3. Plaintiff Has Adequately Alleged That WSOD Acted "Intentionally."**

Plaintiff's CFAA claims all require her to plead that WSOD acted "intentionally" in one form or another. Section 1030(a)(2)(C), for example, prohibits a person from "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer." Similarly, Section 1030(a)(5)(C) prohibits a person from "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss."

WSOD argues that plaintiff has not pled the requisite "criminal intent" on the part of WSOD to satisfy the requirements in CFAA that it act "intentionally." *See* WSOD Mem. at 10. WSOD says that it was at most negligent for failing to track recycled

---

<sup>5</sup> "CAN-SPAM" is short for the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. § 7701 et seq.

wireless telephone numbers and also blames prior owners of those wireless numbers for failing to delete their old numbers from their Watch List Alert accounts. *Id.* at 11. According to WSOD, its reckless or negligent conduct does not rise to the level of intentional conduct. *Id.* However, WSOD cites no cases in support of its argument and for good reason.

There is little authority interpreting CFAA that discusses the *mens rea* required for a person to act “intentionally.” The 1986 Senate Report discussing the 1986 amendments to CFAA, however, sets forth various guiding principles for interpreting the term “intentionally”:

The substitution of an ‘intentional’ standard [in the 1986 amendments] is designed to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files of data belonging to another. Again, this will comport with the Senate Report on the Criminal Code, which states that “‘intentional’ means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person’s conscious objective.”

S. Rep. No. 99-474, 99th Cong. 2nd Sess., U.S. Code Cong. & Admin. News 1986, at p. 2484, Oct. 6, 1986); *see also United States v. Drew*, --- F.R.D. ---, 2009 WL 2872855, \*8 (C.D. Cal. Aug. 28, 2009) (quoting the 1986 Senate Report stating that “intentional acts of unauthorized access – rather than mistaken, inadvertent, or careless ones – are precisely what the Committee intends to proscribe”).

What is relatively settled is CFAA’s “intentional access” provisions do not require a plaintiff to plead that WSOD intentionally damaged her wireless device, *see United States v. Sablan*, 92 F.3d 865, 868 (9th Cir. 1996), or that WSOD “knew the value of the

information obtained.” *United States v. Willis*, 476 F.3d 1121, 1126, 1125 (10th Cir. 2007) (CFAA only requires that the government or plaintiff show “the intent to obtain unauthorized access [to] a protected computer”). *See also Drew*, 2009 WL 2872855, at \*9 (citing the same language in *Willis*).

In *In re Intuit Privacy Litigation*, the Court rejected defendant’s argument on a motion to dismiss that it did not act “intentionally” under CFAA when it “intentionally placed cookies on Plaintiffs’ computers; the cookies allegedly allowed Defendant to retrieve data from Plaintiff’s computers.” 138 F. Supp. 2d 1272, 1280 (C.D. Cal. 2001). Importantly, in *In re Intuit Privacy Litigation*, the Court did not suggest that defendant knew the particular identities of the owners of the computers on which it placed the cookies. *Id.* In addition to *In re Intuit Privacy Litigation*, other courts have held, in albeit in an analogous contexts, that a person acts “intentionally” by “affirmatively directing” electronic communications to the computers or wireless devices of others. *See Compuserve Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (in context of state-law claim for trespass to chattels for unsolicited “spam” e-mail, defendant acted “intentionally” by “affirmatively directing” unsolicited e-mail to unknown recipients with Compuserve e-mail accounts).

Here, as an initial matter, WSOD’s argument that plaintiff did “not allege that WSOD intentionally accessed her cell phone” borders on frivolous. *See* WSOD Mem. at 10. Plaintiff’s second amended complaint is replete with allegations that WSOD acted “intentionally.” *E.g.*, 2d Am. Compl. at ¶¶ 94, 98-99. Second, although plaintiff believes and therefore avers in her second amended complaint that WSOD acted with the requisite

intent, such intent generally can only be proven through discovery, which discovery WSOD has objected to producing while this Court resolves the instant motion to dismiss. *See* Order of Sept. 15, 2009, Docket No. 36 (Erickson, M.J.) (observing that WSOD had asked “that [the Court] stay discovery until the District Court rules on the pending Motion to Dismiss”); *cf. Estate of Klieman v. Palestinian Auth.*, 424 F. Supp. 2d 153, 167 (D.D.C. 2006) (holding that the court could not “determine defendants’ intent . . . in the context of a motion to dismiss; that is a question for trial or, at a minimum, for summary judgment”).

Finally, although WSOD claims that it only acted negligently or recklessly in initially sending unauthorized text messages to plaintiff’s wireless device, it has no response whatsoever to plaintiff’s allegations that she continued to receive text messages from WSOD after she complained to WSOD about the text messages, *see* 2d Am. Compl. at ¶¶ 77-78, and concedes that plaintiff has alleged that it finally stopped sending text messages to plaintiff only after it heard from plaintiff’s lawyer. *See* WSOD Mem. at 9. Once plaintiff put WSOD on explicit notice that it was sending her text messages she neither authorized nor wanted to receive, it is reasonable to infer from the allegations in the second amended complaint that WSOD’s acts of continuing to send unauthorized text messages to plaintiff’s wireless device were done “intentionally.” *See Czech*, 2009 WL 2045308, \*1 (on a motion to dismiss, the court should assume “all facts in the complaint

to be true and construe[] all reasonable inferences from those facts in the light most favorable to the complainant” (citation omitted)).<sup>6</sup>

**4. Plaintiff Adequately Alleged That WSOD “Obtained Information” From Her Wireless Device.**

Section 1030(a)(2)(C) requires plaintiff to plead that WSOD “obtain[ed] information” from her wireless device. The threshold for alleging that a person “obtained information” under CFAA is minimal, especially considered in conjunction with Rule 12’s notice-pleading rules:

The Department of Justice has expressed concerns that the term “obtains information” in 18 U.S.C. § 1030(a)(2) makes that subsection more than an unauthorized access offense, i.e., that it might require the prosecution to prove asportation of data in question. Because the premise of this subsection is privacy protection, the Committee wishes to make clear that “obtaining information” in this context includes mere observation of the data. Actual asportation, in the sense of physically removing the data from its original location or transcribing the data, need not be proved in order to establish a violation of this subsection.

S. Rep. No. 99-474, 99th Cong. 2nd Sess., U.S.Code Cong. & Admin. News 1986, at p. 2484, Oct. 6, 1986) (emphases added); *see also Drew*, 2009 WL 2872855, at \*6 (quoting same language). The term “obtaining information,” therefore, includes “merely reading” the information:

“Information” as used in this subsection includes information stored in intangible form. Moreover, the term “obtaining information” includes merely reading it. There is no requirement that the information be copied or transported.

---

<sup>6</sup> The same principles apply to plaintiff’s claims under Section 1030(a)(5)(A), which requires plaintiff to show that WSOD “intentionally cause[d] damage without authorization” to her wireless device.

S. Rep. No. 104-357, 104th Cong. 2nd Sess., 1996 WL 492169, \*7 (Aug. 27, 1996); *see also Drew*, 2009 WL 2872855, at \*6 n.13 (quotations omitted). Merely accessing a publicly available Internet website, for example, without more, satisfies CFAA's "obtains information" element. *Drew*, 2009 WL 2872855, at \*6, 16; *cf. LCGM, Inc.*, 46 F. Supp. 2d at 450 (stating that obtaining e-mail addresses constitutes "obtaining information" under CFAA).

In this Court's prior Order denying WSOD's initial motion for judgment on the pleadings, the Court voiced its concern that the allegations in the first amended complaint were "insufficient to allege that WSOD actually obtained information from Czech's cell phone" because there were no allegations in the amended complaint "concerning how WSOD gained information from Czech, even assuming her cell phone was slowed or its memory depleted." *Czech*, 2009 WL 2045308, at \*4. This Court also queried "how [the] consumption of a cell phone carrier's bandwidth results in the obtaining of information about an end-user from his or her device." *Id.*

Plaintiff submits that the allegations in the second amended complaint are sufficient to address the Court's concerns regarding the sufficiency and plausibility of plaintiff's claims that WSOD "obtain[ed] information" from her wireless device. The parties, during the briefing on WSOD's initial motion for judgment on the pleadings, admittedly were operating under the belief that CFAA required plaintiff to plead that WSOD accessed and then removed or took tangible information from plaintiff's wireless device. WSOD continues to operate under that assumption; it argues in its brief that a plain reading of the "obtains-information" requirement, as well as the case law

interpreting that requirement, shows “that information must actually be obtained *from the computer*.” WSOD Mem. at 11, 12 n.12 (citing cases holding that actually removing data from a protected computer constituted “obtaining information”). Nonetheless, as the 1986 Senate Report and case law above make clear, CFAA does not require “[a]ctual asportation, in the sense of physically removing the data from its original location or transcribing the data . . . to establish a violation of” Section 1030(a)(2)(C); *see also Drew*, 2009 WL 2872855, at \*6 n.13, 16. (a person “obtains information” by “merely reading” the information).

Even if CFAA requires WSOD to have actually obtained tangible information (as in actually removing or taking information) from plaintiff’s wireless device, as opposed to merely observing data (which it does not), plaintiff’s allegations in the second amended complaint satisfy that heightened test as well. The second amended complaint contains myriad allegations of the tangible information actually obtained by WSOD from plaintiff’s wireless device:

- If a text message is successfully sent to a wireless device, as opposed to being “bounced back” from the user-recipient (similar to an undeliverable e-mail), the person sending the text message obtains information (through a read- or delivery-receipt or other delivery notification) that the wireless number is active, the general geographic area where the user is located (via the information obtained through simple analysis of the wireless number’s area code), and that future text messages can be sent to that active wireless number, 2d Am. Compl. at ¶ 45; *see also* 2d Am. Compl. at ¶ 96;
- Knowing that a particular wireless number is active and the general or actual geographic location of the wireless-device user, including Plaintiff and the members of the Class, also allows the sender of a text message, such as WSOD, to sell, license, or otherwise market

that wireless number to others, including clients or affiliates of the sender, such as those clients or affiliates contracting with WSOD, who wish to send related text-message content to that active wireless number, 2d Am. Compl. at ¶ 46;

- The information obtained by senders of text messages such as WSOD who determine that a wireless-number is active also allows commercial senders of text messages, such as WSOD, to evade the restrictions on making unsolicited commercial-marketing telephone calls to wireless numbers registered on the government's "Do Not Call" list and lets senders such as WSOD circumvent the restrictions on sending unauthorized text messages under the CAN-SPAM Act, 2d Am. Compl. at ¶ 47;
- By sending unauthorized text messages to Plaintiff's cellular telephone, WSOD obtained information that Plaintiff's cellular telephone was active and functioning, and obtained information regarding the general and/or actual geographic location of Plaintiff's cellular telephone, 2d Am. Compl. at ¶ 73;
- WSOD also knowingly obtained information from Plaintiff's cellular telephone in the form of obtaining a portion of the finite permanent or hard drive memory storage capacity of the phone, 2d Am. Compl. at ¶ 74; *see also* 2d Am. Compl. at ¶ 97.

WSOD nevertheless contends that even if it did "obtain information" from plaintiff's wireless device in the form of an electronic confirmation that her wireless number was active and that future text messages could be sent to the device, it did not really obtain any new information because it "already knew the number was active" because it "had been receiving delivery or receipt confirmations even before the number was 'recycled' to Plaintiff." WSOD Mem. at 13-14. WSOD also argues that it could not have obtained information from plaintiff's wireless device about the general geographic area where plaintiff was located "because that area code was also known to WSOD when the subscriber signed up for the service." *Id.* at 14. The problem with these arguments –

which are premised on disputed factual assertions concerning what WSOD knew and when – is that they contradict the allegations in plaintiff’s second amended complaint; as such, WSOD’s own version of the facts cannot be considered on a motion to dismiss, where all of plaintiff’s allegations, and the reasonable inferences from those allegations, must be taken as true by this Court.

In summary, WSOD’s argument that it did not obtain information from plaintiff’s wireless device because “it is not enough to ‘access information’” and that “the CFAA requires that the violator *actually take possession of information* from the computer” is based on a faulty assumption that this is the proper test under the statute. *See* WSOD Mem. at 15. It is not. Because “[a]ctual asportation, in the sense of physically removing the data from its original location or transcribing the data, need not be proved in order to establish a violation of” Section 1030(a)(2)(C), plaintiff has properly stated a claim under that subsection of CFAA.

**5. Plaintiff Has Adequately Alleged That WSOD Caused Damage To Her Wireless Device.**

Two of plaintiff’s CFAA claims require her to plead that WSOD caused “damage” to her wireless device. 28 U.S.C. § 1030(a)(5)(A) requires plaintiff to plead that WSOD “knowingly cause[d] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[d] damage without authorization” to her wireless device. 28 U.S.C. § 1030(a)(5)(C) requires plaintiff to plead that WSOD “intentionally accesse[d]” her wireless device “without authorization,” as a result of such conduct “intentionally cause[d] damage and loss.” CFAA defines “damage” as “any

*impairment to the integrity or availability of data, a program, a system, or information.*” 18 U.S.C. § 1030(e)(8) (2008) (emphases added).

In its Order denying WSOD’s initial motion for judgment on the pleadings, this Court, focusing only on paragraph 24 of the first amended complaint, concluded that plaintiff’s allegations “do not explain how Czech or the proposed class members suffered any damage. Instead the allegations in the Amended Complaint are merely conclusory statements listing generalized grievances that are insufficient under *Twombly*.” *Czech*, 2009 WL 2045308, at \*4.

In her second amended complaint, however, plaintiff has expanded her allegations regarding the damage caused by WSOD to her wireless device, and to the wireless devices of the members of the Class. In her second amended complaint, plaintiff alleges the following, among other things, with regard to herself and the similarly situated members of the Class:

- Handheld wireless devices, in contrast to modern personal computers, have relatively limited random-access or random-operating memory (“RAM” or “ROM”). When a wireless device receives an unauthorized text message, the wireless device’s finite RAM or ROM is depleted or “used up,” causing the device’s other electronic operations and functioning (including the user’s receipt of legitimate text-message content) to slow or lag in operation, or actually lock up completely, 2d Am. Compl. at ¶ 27;
- Unauthorized text messaging, such as the text messaging by WSOD, also can cause a wireless device to shut down completely and automatically reset, with the result being the device rebooting itself, reformatting the memory of wireless device, and erasing any stored information on the device’s permanent storage or “hard drive,” 2d Am. Compl. at ¶ 28;

- When a wireless device is in the process of receiving an unauthorized text message, wireless bandwidth that would otherwise be dedicated to other wireless operations such as the user's telephone calls, internet access, instant messaging, or the user himself sending or receiving a legitimate text message, is misallocated, interfered with, and/or depleted, 2d Am. Compl. at ¶ 28;
- Handheld wireless devices, unlike modern personal computers, also have relatively finite permanent or "hard drive" memory storage capacity. Consequently, the more unauthorized text messages a wireless device receives the more finite hard drive storage capacity of a wireless device is temporarily and/or permanently misallocated, depleted, or consumed, which causes, among other things, the wireless device to slow or lag in its operation or functioning, or otherwise shutdown completely, 2d Am. Compl. at ¶ 31;
- The unauthorized text messages Plaintiff received from WSOD depleted or "used up" the phone's finite RAM or ROM and caused the phone's electronic operations and functioning to slow and lag in operation and functioning, 2d Am. Compl. at ¶ 70 (emphasis added);
- The unauthorized text messages Plaintiff received from WSOD also resulted in the misallocation, interference, or depletion of Plaintiff's cellular telephone's limited wireless bandwidth that would otherwise have been dedicated to Plaintiff's other wireless operations such as Plaintiff's incoming and outgoing telephone calls, internet access, instant messaging, and Plaintiff's own sending or receiving of legitimate text messages, 2d Am. Compl. at ¶ 71 (emphases added);
- The unauthorized text messages Plaintiff received from WSOD also resulted in the temporary and/or permanent misallocation, depletion, or consumption of Plaintiff's cellular telephone's finite permanent or "hard drive" memory storage capacity, which also caused Plaintiff's cellular telephone to slow or lag in its operation and functioning, 2d Am. Compl. at ¶ 72 (emphases added);
- The unauthorized text messages Plaintiff and the members of the Class received from WSOD caused damage to Plaintiff's cellular telephone and the wireless devices of the members of the Class by depleting or "using up" the wireless devices' finite RAM or ROM

causing the electronic operations and functioning of the wireless devices to slow or lag in operation, 2d Am. Compl. at ¶ 100 (emphases added);

- The unauthorized text messages Plaintiff received from WSOD also caused damage to Plaintiff's cellular telephone and the wireless devices of the members of the Class by misallocating, interfering, or depleting the limited wireless bandwidth of the wireless devices that would have otherwise been dedicated to other wireless operations such as the telephone calls, internet access, instant messaging, or the sending or receiving of legitimate text messages by Plaintiff and the members of the Class, 2d Am. Compl. at ¶ 101 (emphases added);
- The unauthorized text messages Plaintiff received from WSOD also caused damage to Plaintiff's cellular telephone and the wireless devices of the members of the Class by temporarily and/or permanently misallocating, depleting, or consuming the finite permanent or "hard drive" memory storage capacity of Plaintiff's cellular telephone and the wireless devices of the members of the Class, which caused Plaintiff's cellular telephone and the wireless devices of the members of the Class to slow or lag in operation and functioning, 2d Am. Compl. at ¶ 102 (emphases added);

As plaintiff noted in her memorandum opposing WSOD's initial motion for judgment on the pleadings, courts have held in similar circumstances that damage under CFAA can be found where unwanted electronic communications causes a computer to slow or otherwise diminish the capacity of the computer to function. *See Am. Online, Inc. v. Nat'l Health Care Discount, Inc.*, 121 F. Supp. 2d 1255, 1274 (N.D. Iowa 2000) (holding that "when a large volume of [e-mail] causes slowdowns or diminished the capacity of [a protected computer] an 'impairment' has occurred to the 'availability' of [a] 'system'" (quotation omitted)); *see also Am. Online, Inc. v. Prime Data Sys., Inc.*, No. Civ.A. 97-1652-A, 1998 WL 34016692, \*3 (E.D. Va. Nov. 20, 1998) (finding as one

element of damages under CFAA the value of computer capacity tied up by defendant's unsolicited bulk e-mail activities).

What WSOD is actually arguing – though it does not state it explicitly – is that there is some kind of *de-minimus* or nominal-damage exception to CFAA's "damage" requirements. WSOD, however, does not make this argument explicitly because there is no such exception. *See* 18 U.S.C. § 1030(e)(8) (defining "damage," in part, as "any impairment" (emphasis added)). Nor has any case recognized such a *de-minimus* or nominal-damage exception. *See Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 251 (S.D.N.Y. 2000) (holding that defendant's unauthorized use of search robots "has diminished server capacity, however slightly, and could diminish response time, which *could* impair the availability of data" (emphases added)), *aff'd*, 356 F.3d 393 (2d Cir. 2004).

**C. Plaintiff Has Stated A Claim For Common-Law Trespass To Chattels.**

**1. WSOD Performs No Choice-Of-Law Analysis For Plaintiff's Claim For Trespass To Chattels.**

As it did in its initial motion for judgment on the pleadings, WSOD again fails to discuss the choice-of-law issues applicable to Plaintiff's common-law claims for trespass to chattels (and unjust enrichment, discussed below), and simply assumes once again that Minnesota law applies to those claims. *See* WSOD Mem. at 9, 15-19. This failure alone is sufficient reason to deny its motion as to these claims.<sup>7</sup>

---

<sup>7</sup> *See Harper v. LG Elecs. USA, Inc.*, 595 F. Supp. 2d 486, 490 (D.N.J. 2009) (denying defendant's motion to dismiss because the court was "unable to make the intensive choice-of-law determination on the record before it" and deferring the issue to

Either Minnesota law, Colorado law, or possibly other state law might apply to Plaintiff's common-law claims for trespass to chattels, depending on the facts adduced during discovery. Plaintiff is a resident of Minnesota. WSOD is located in and does business in Colorado, but it also conducts business throughout the United States. *See Answer to First Amended Complaint* ¶ 10. WSOD's failure to conduct any choice-of-law analysis regarding Plaintiff's common-law claim for trespass to chattels leaves unclear what state's law applies to this claim and, once again, is grounds for denial of its motion to dismiss plaintiff's claim for trespass to chattels.

## **2. Plaintiff Alleges The Elements Of A Claim For Trespass To Chattels.**

In its initial motion for judgment on the pleadings, WSOD argued that Minnesota law does not recognize the common-law tort of trespass to chattels. It has abandoned that argument in its instant motion. Instead, WSOD now argues that Minnesota courts only recognize the tort of trespass to chattels found in the Restatement (Second) of Torts § 222. *See WSOD Mem.* at 18. According to WSOD, plaintiff has not stated a claim

---

the summary judgment stage); *Taylor v. JVC Americas Corp.*, No. 07-4059, 2008 WL 2242451, \*4 n.3 (D.N.J. May 30, 2008) (denying defendant's motion to dismiss statutory consumer-fraud claim because "the parties have failed to address . . . the Court's choice-of-law analysis," which alone was sufficient to deny the motion to dismiss); *Waldock v. M.J. Select Global, LTD.*, No. 03 C 5293, 2005 WL 3542527, \*14 (N.D. Ill. Dec. 27, 2005) (denying defendants' motion to dismiss breach-of-contract claim noting that defendants assumed that Bahamian law applied to the claim without engaging in any choice-of-law analysis and thus "failed to lay the proper ground work [sic] for the court to address their argument" (quotation omitted)); *In re Air Crash Disaster at Sioux City, Iowa on July 19, 1989*, No. 90-2255, 1991 WL 268656, \*2 (N.D. Ill. Dec. 4, 1991) (same).

under Section 222 because she has not alleged that “WSOD took actual possession of her phone.” *Id.* (“Plaintiff does not allege that WSOD actually took her cell phone.”).

WSOD now correctly concedes that Minnesota courts do recognize some form of the common-law tort of trespass to chattels. *See Herrmann v. Fossum*, 270 N.W.2d 18, 20-21 (Minn. 1978) (holding that plaintiff stated a claim for trespass to chattels and citing to Restatement (Second) of Torts § 222 (1965), which provides: “One who dispossesses another of a chattel is subject to liability in trespass for the damage done”); *Wells Elec., Inc. v. Schaper*, No. A-06-420, 2006 WL 2807179, \*5-6 (Minn. Ct. App. Oct. 3, 2006) (reversing district court’s grant of summary judgment on plaintiff’s claim for trespass to chattels because disputed questions of fact existed, citing the elements of the tort found in Restatement (Second) of Torts § 222 (1965)).

But Minnesota courts have never held that the common-law tort of trespass to chattels is cabined by Restatement (Second) of Torts § 222, or that an actual taking of a chattel is required to state a claim under that section. Section 222 does not provide that an “actual taking” is required to bring a claim for trespass to chattels; rather, it only vaguely requires a “dispossession.” In addition, Restatement (Second) of Torts § 217 provides that a “trespass to chattel may be committed by intentionally (a) dispossessing another of the chattel, or (b) using or intermeddling with a chattel in the possession of another.” (Emphasis added.)

With regard to the sufficiency of plaintiff’s allegations in support of her claim for trespass to chattels, they are more than sufficient to satisfy the requirement of dispossession or the “using or intermeddling with a chattel in the possession of another”

under Minnesota or Colorado<sup>8</sup> law. Plaintiff alleges, for example, that WSOD's text messages:

- (1) depleted or "used up" the finite RAM or ROM of the wireless devices causing the electronic operations and functioning of the wireless devices to slow or lag in operation; (2) misallocated, interfered with, or depleted the limited wireless bandwidth of the wireless devices that otherwise would have been dedicated to other wireless operations of Plaintiff and the members of the Class such as telephone calls, internet access, instant messaging, and/or the sending or receiving of legitimate text messages; and (3) temporarily and/or permanently misallocated, depleted, or consumed the finite permanent or "hard drive" storage capacity of Plaintiff's cellular telephone and the wireless devices of the members of the Class, which caused Plaintiff's cellular telephone and the wireless devices of the members of the Class to slow or lag in operation or functioning, 2d Am. Compl. at ¶ 109.

Finally, as plaintiff pointed out in opposing WSOD's initial motion for judgment on the pleadings, several federal district courts and at least one court of appeal have concluded that a plaintiff can bring a claim for trespass to chattels in the context of the transmission of unsolicited e-mails, spyware, search robots, web spiders, and other automated-data-collection and electronic-scraping devices under various states' common laws. *See Sotelo v. DirectRevenue, LLC*, 384 F. Supp. 2d 1219, 1229-31 (N.D. Ill. 2005) (denying defendant's motion to dismiss trespass-to-chattels claim under Illinois law and noting that plaintiff had adequately alleged that defendant's spyware "interfered with and damaged his personal property, namely his computer and his Internet connection, by

---

<sup>8</sup> Colorado courts, too, recognize the tort of trespass to chattels. *See Mountain States Tel. & Tel. Co. v. Horn Tower Constr. Co.*, 363 P.2d 175, 177 (Colo. 1961) ("Trespass to chattels is defined as the intentional interference with the possession, or physical condition of a chattel in the possession of another without justification.").

over-burdening their resources and diminishing their functioning”).<sup>9</sup> As the Court in *Register.com, Inc. v. Verio, Inc.*, observed, although evidence of any burden or harm to a computer system may be imprecise, “evidence of mere possessory interference is sufficient to demonstrate the quantum of harm necessary to establish a claim for trespass to chattels.” 126 F. Supp. 2d 238, 250 (S.D.N.Y. 2000), *aff’d*, 356 F.3d 393 (2d Cir. 2004).

---

<sup>9</sup> See *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 404-05 (2d Cir. 2004) (applying New York law and upholding grant of preliminary injunction on claim for trespass to chattels to stop defendant’s use of search robots targeting plaintiff’s computer systems); *State Analysis, Inc. v. Am. Fin. Servs. Assoc.*, No. 1:08cv1333, 2009 WL 855793, \*7 (E.D. Va. Mar. 31, 2009) (applying Virginia law); *Southwest Airlines Co. v. Farechase, Inc.*, 318 F. Supp. 2d 435, 442 (N.D. Tex. 2004) (applying Texas law; denying motion to dismiss trespass to chattels claim arising from defendant’s use of search robots or scraping devices); *Am. Online, Inc. v. Nat’l Health Care Discount, Inc.*, 121 F. Supp. 2d 1255, 1277 (N.D. Iowa 2000) (applying Virginia law); *eBay Inc. v. Bidder’s Edge, Inc.*, 100 F. Supp. 2d 1058, 1064-73 (N.D. Cal. 2000) (enjoining defendant from accessing eBay’s computer systems using automated querying program without eBay’s prior authorization); *Am. Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 451-52 (E.D. Va. 1998) (applying Virginia law; citing cases and denying defendant’s motion for summary judgment on plaintiff’s trespass-to-chattels claim and noting that “[c]ourts have recognized that the transmission of unsolicited bulk e-mails can constitute a trespass to chattels”); *Am. Online, Inc. v. IMS*, 24 F. Supp. 2d 548, 550-51 (E.D. Va. 1998) (applying Virginia law; sending bulk “spam” e-mail constituted trespass to chattels); *Hotmail Corp. v. Van\$ Money Pie, Inc.*, No. C 98-20064 JW, 1998 WL 388389, \*7 (N.D. Cal. Apr. 16, 1998) (applying California law; sending bulk “spam” e-mail constituted trespass to chattels); *Am. Online v. Prime Data Sys., Inc.*, No. Civ.A. 97-1652-A, 1998 WL 34016692, \*3 (E.D. Va. Nov. 20, 1998); *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1021-24 (S.D. Ohio 1997) (holding that physical dispossession of a chattel is not required to state a claim for trespass to chattels where the quality, condition, or value of the computer services were harmed as a result of defendant’s conduct).

**D. Plaintiff States A Claim For Unjust Enrichment.****1. WSOD Performs No Choice-Of-Law Analysis For Plaintiff's Claims For Unjust Enrichment.**

As discussed above, this Court should deny WSOD's motion to dismiss plaintiff's common-law claims for unjust enrichment because WSOD has not even attempted a choice-of-law analysis to determine which state's law applies to plaintiff's claim, which should be especially fatal on a motion to dismiss.

**2. Plaintiff Adequately Alleges The Elements Of A Claim For Unjust Enrichment.**

WSOD contends, as it did before, that Plaintiff "must allege that WSOD retained a benefit, that doing so is unjust in the sense that unjust could mean illegally or unlawfully, and that WSOD did so at [Plaintiff's] expense." WSOD Mem. at 20. WSOD argues that "Plaintiff does not allege that she incurred any additional expenses beyond what she was paying [for her monthly text-messaging plan] or even that she had to restrict her text message usage because of WSOD's text messages." *Id.* at 21. WSOD says that there is no way it could have "received something of value by depleting the number of Plaintiff's text messages that would otherwise be left in her [monthly text-messaging plan]." *Id.*

In her second amended complaint, however, plaintiff alleged just how WSOD was enriched at plaintiff's expense. As for how plaintiff suffered an "expense," little needs to be said. Plaintiff paid a monthly fee for a text-messaging plan that limited her to sending and receiving a certain number of text messages. The cost to plaintiff of each text message sent and received, therefore, is quantifiable – it is the cost of plaintiff's monthly text-messaging plan divided by the number of text messages she could send or receive

under the plan. By sending plaintiff unauthorized text messages to plaintiff's wireless device, WSOD necessarily depleted the number of available text messages plaintiff could send or receive per month from legitimate sources, and plaintiff therefore suffered an "expense" equal to the number of unauthorized text messages she received from WSOD multiplied by the cost per text message under her text-messaging plan. *See* 2d Am. Compl. at ¶ 116.

As for how WSOD was enriched by sending plaintiff unauthorized text messages, the picture becomes even clearer. In her second amended complaint, plaintiff alleges that WSOD's sends Watch List Alert text messages (both authorized and unauthorized) on behalf of its institutional clients to make money. Why else would WSOD offer this text-messaging business platform to its institutional clients and Watch List Alert customers if not to make a profit? After all, it would make no business or economic sense for WSOD to offer text-messaging functionality to its institutional clients and its Watch List Alert customers for free.

Therefore, as plaintiff alleges in her second amended complaint,

Defendants have been unjustly enriched at Plaintiff's and the Class's expense as the result of the text message fees generated by WSOD by sending unauthorized text messages to Plaintiff and the members of the Class, and the unlawfully retained profit made by WSOD from its text-messaging-content contracts with its clients and affiliates, which contracts were premised on sending as many text messages as possible to wireless-device users despite the fact that WSOD knew that many of these users never authorized WSOD to send them text messages.

2d Am. Compl. at ¶ 115. Put together, plaintiff's expense (the depletion of the number of available text messages in her monthly plan) and WSOD's enrichment at plaintiff's

expense (its profit from sending as many text messages as possible regardless of whether they were authorized or not) satisfies the requirements for stating a claim for unjust enrichment, regardless of which state's law applies.

WSOD calls these particular allegations a "vague conspiracy theory"; they are anything but. These allegations are based on reasonable inferences plaintiff has made from her understanding (which is necessarily limited because of WSOD's refusal to produce even limited discovery) of how WSOD's so-called "business" works. Nothing more is required of plaintiff under *Twombly* and *Iqbal*.

**3. CFAA Does Not Provide Plaintiff An Adequate Remedy At Law Precluding Plaintiff's Common-Law Claim For Unjust Enrichment.**

As it did in its initial motion for judgment on the pleadings, WSOD argues that plaintiff's claim for unjust enrichment is precluded by the "very existence" of CFAA because CFAA provides plaintiff an "adequate remedy at law." WSOD Mem. at 22. WSOD claims that it doesn't matter that plaintiff cannot prevail on her CFAA claim because "CFAA provides a cause of action for the type of conduct alleged in this case." *Id.* at 23.

**a) Plaintiff's claim for unjust enrichment is not precluded by the "very existence" of CFAA because she may plead alternative, even inconsistent, causes of action.**

WSOD's argument ignores plaintiff's right to plead alternative, even inconsistent, causes of action at this early stage of the proceedings. *See, e.g.,* Fed. R. Civ. P. 8(a)(2)-(3). What is more, none of the federal courts that have entertained claims for unjust

enrichment along with claims under CFAA have suggested that CFAA preempts or otherwise prevents a plaintiff from bringing such a common-law claim. *See State Analysis, Inc. v. Am. Fin. Servs. Assoc.*, No. 1:08cv1333, 2009 WL 855793, \*10 (E.D. Va. Mar. 31, 2009) (applying Virginia law); *Oracle Corp. v. SAP AG*, No. C 07-1658, 2008 WL 5234260, \*9 (N.D. Cal. Dec. 15, 2008) (refusing to dismiss claim for unjust enrichment “simply because it conflicts with another cause of action” and noting that “plaintiffs are entitled to plead inconsistent causes of action” under Fed. R. Civ. P. 8(a)(2)); *Binary Semantics Ltd. v. Minitab, Inc.*, No. 4:07-CV-1750, 2008 WL 763575, \*5, 9-10 (M.D. Pa. Mar. 20, 2008) (denying defendants’ motion to dismiss plaintiff’s CFAA claim and unjust-enrichment claim and holding that the Pennsylvania Uniform Trade Secrets Act did not displace the unjust-enrichment claim).

Nonetheless, WSOD claims in a footnote that “[t]his is not a situation where Plaintiff is free to plead unjust enrichment in the alternative. Under this view, every failed statutory claim would yield a claim in equity.” WSOD Mem. at 24 n.5. WSOD cites *Frank v. Gold’n Plump Poultry, Inc.*, No. 04-CV-1018, 2007 WL 2780504, \*11 (D. Minn. Sept. 24, 2007) (Schiltz, J.) for this contention; however, *Frank* does not address this argument, much less resolve it. Notably, WSOD cites no other case in support of its argument that plaintiff is not able to plead alternative, even inconsistent, causes of action. This Court should, therefore, deem this particular argument waived by WSOD, and not allow it to revive it in its reply. *See Chay-Velasquez v. Ashcroft*, 367 F.3d 751, 756 (8th Cir. 2004) (“Since there was no meaningful argument on this claim in [the] opening brief, it is waived.”).

**b) Plaintiff's claim for unjust enrichment is not precluded by the "very existence" of CFAA because each particular legal claim seeks different forms of relief.**

Assuming Minnesota law<sup>10</sup> applies here, it does not preclude Plaintiff's unjust-enrichment claim, because Plaintiff's CFAA claim and her unjust-enrichment claim seek different forms of relief for different injuries suffered by Plaintiff as a result of WSOD's unlawful conduct. *See Hecht v. Components Int'l, Inc.*, 867 N.Y.S.2d 889, 898 (N.Y. Sup. Ct. 2008) ("It appears that the CFAA is not intended to preempt state law claims based on unauthorized access to a computer such as trespass to chattel, conversion, or

---

<sup>10</sup> The plethora of Minnesota decisions WSOD cites are so far afield, Plaintiff will only briefly summarize their non-applicability and other infirmities here. *See Servicemaster of St. Cloud v. GAB Bus. Servs', Inc.*, 544 N.W.2d 302, 305-06 (Minn. 1996) (reversing damages award for unjust enrichment because plaintiff failed to file required statutory pre-lien notice and could have proceeded under a constitutional-lien theory); *United States Fire Ins. Co. v. Minn. State Zoological Bd.*, 307 N.W.2d 490, 497 (Minn. 1981) (claim for unjust enrichment precluded because rights of parties were governed by a contract and "constitutional and statutory restrictions on the State's ability to pay money from the general fund would be circumvented"); *Stocke v. Berryman*, 632 N.W.2d 242, 245-46 (Minn. Ct. App. 2001) (equitable relief denied because plaintiffs had a remedy under Minn. Stat. § 423B and corporate bylaws); *Breezy Point Holiday Harbor Lodge Beachside Apartment Owners' Ass'n v. B.P. P'ship*, No. C0-96-59, 1996 WL 422562, \*2 (Minn. Ct. App. July 30, 1996) (affirming denial of claim for unjust enrichment because plaintiff had an adequate remedy at law under Minn. Stat. § 515.07); *Airlines Reporting Corp. v. Norwest Bank, N.A.*, 529 N.W.2d 449, 452 (Minn. Ct. App. 1995) (denying request for equitable estoppel where U.C.C. provided adequate remedy at law); *Southtown Plumbing, Inc. v. Har-Ned Lumber Co.*, 493 N.W.2d 137, 140 (Minn. Ct. App. 1992) (holding that plaintiff could not recover under unjust-enrichment theory where it failed to pursue a statutory mechanics lien or breach-of-contract claim); *Zimmerman v. Lasky*, 374 N.W.2d 212, 215 (Minn. Ct. App. 1985) (affirming denial of injunctive relief seeking to restrain court from holding plaintiff in contempt of court where plaintiff failed to appeal his conviction under Minn. R. Crim. P. 28.01); *Northwoods Env't'l Inst. v. Minn. Pollution Control Agency*, 370 N.W.2d 449, 451 (Minn. Ct. App. 1985) (refusing to grant an extraordinary writ of mandamus because plaintiff had an adequate remedy at law).

fraud.” (citing *Pacific Aerospace & Electronics v. Taylor*, 295 F. Supp. 2d 1188, 1194 (E.D. Wash. 2003)).

Plaintiff’s CFAA claim and her trespass-to-chattels claim primarily seek relief for WSOD’s unauthorized access, occupation, interruption of service, depletion of memory, impairment, and dispossession of Plaintiff’s cellular telephone. Plaintiff’s unjust-enrichment claim, however, seeks relief for the expense incurred by plaintiff as the result of the depletion of her monthly text-messaging plan as well as the economic benefit conferred on WSOD as the result of its sending unauthorized text messages to plaintiff’s wireless device and the wireless devices of the members of the Class. *See supra* Section II.D.2. WSOD fails to show that CFAA would allow Plaintiff recovery for this latter type of damages. *See A.V. by Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 645-46 (4th Cir. 2009) (discussing the potential types of “economic damages” including consequential damages cognizable under CFAA).

Consequently, WSOD’s reliance on cases such as *Smith v. Sprague*, 143 F.2d 647, 650 (8th Cir. 1944) (denying equitable relief where no legal right to recovery existed at all under the law) to show that plaintiff has an adequate remedy at law is simply unavailing. *See also Frank v. Gold’n Plump Poultry, Inc.*, No. 04-CV-1018, 2007 WL 2780504, \*11 (D. Minn. Sept. 24, 2007) (Schiltz, J.) (dismissing on summary judgment plaintiff’s claims for unjust enrichment because state and federal labor laws provided plaintiffs with a remedy *if* defendant wrongfully underpaid them); *Arena Dev. Group, LLC v. Naegele Communications, Inc.*, No. 06-2806, 2007 WL 2506431, \*11 (D. Minn. Aug. 30, 2007) (dismissing plaintiffs’ claim for unjust enrichment because claim for

fraudulent conveyances were governed *exclusively* by the Uniform Transfers Act, which provided the exclusive remedy for recovery).

**E. If This Court Dismisses Plaintiff's Claims Under CFAA, It Should Not Exercise Supplemental Jurisdiction To Decide Whether Plaintiff Has Stated Claims For Trespass To Chattels And Unjust Enrichment.**

WSOD argues, as it did before, that this Court should exercise its supplemental jurisdiction and dismiss plaintiff's state-law claims even if it first dismisses plaintiff's claims under CFAA. *See* WSOD Mem. at 24.

If this Court decides to dismiss plaintiff's CFAA claims, however, it should decline to rule on WSOD's motion to dismiss plaintiff's state-law claims; instead, this Court should dismiss those state-law claims without prejudice so that Plaintiff can re-file this action in state court. *See* 28 U.S.C. § 1367(c)(3); *see also Carlsbad Tech., Inc. v. HIF Bio, Inc.*, 556 U.S. ---, 129 S. Ct. 1862, 2009 WL 1174837, \*3 (May 4, 2009) ("A district court's decision whether to exercise [supplemental] jurisdiction after dismissing every claim over which it had original jurisdiction is purely discretionary."); *ES & H, Inc. v. Allied Safety Consultants, Inc.*, No. 3:08-cv-323, 2009 WL 2996340, \*4 (E.D. Tenn. Sept. 16, 2009) (dismissing plaintiff's CFAA for failure to plead the requisite "loss" under the statute and dismissing plaintiff's state-law claim "without prejudice to refile the same in an appropriate state court"); *Condux Int'l, Inc.*, 2008 WL 5244818, at \*6 (dismissing with prejudice plaintiff's CFAA claim and declining to exercise supplemental jurisdiction under 28 U.S.C. § 1367(c)(3) over plaintiff's remaining state-law claims).

As this Court itself recognized during the hearing on WSOD's initial motion for judgment on the pleadings, federal courts are courts of limited jurisdiction. *See United*

*Mine Workers of Am. v. Gibbs*, 383 U.S. 715, 726 (1996) (stating that “if the federal claims are dismissed before trial . . . the state claims should be dismissed as well”). Retaining supplemental jurisdiction over plaintiff’s remaining state-law claims, in light of the novel and fact-intensive issues raised by those claims, may result in this Court needlessly rendering a decision on unsettled state law. *See ACLU v. City of Florissant*, 186 F.3d 1095, 1099 (8th Cir. 1999).

### III. CONCLUSION

Judge Easterbrook put it best when he observed that CFAA is a broadly worded statute, and that “[a]s more devices come to have built-in intelligence, the effective scope of the statute grows. This might prompt Congress to amend the statute” but that “does not authorize the judiciary to give [CFAA] less coverage than its language portends.” *United States v. Mitra*, 405 F.3d 492, 495 (7th Cir. 2005). So, too, in this case.

Plaintiff has adequately stated claims under CFAA. She has adequately alleged that WSOD acted “without authorization” when accessing her wireless device; she has adequately alleged that WSOD acted intentionally in doing so; and she has adequately alleged that WSOD obtained information and caused damage to her wireless device. She also has adequately stated state-law claims for trespass to chattels and unjust enrichment, regardless of which particular state’s law applies. And she has done all of this while keeping in mind *Twombly* and *Iqbal*’s admonitions that mere threadbare recitations of the elements of a cause of action no longer suffice to state claims under Rule 12, but that neither *Twombly* nor *Iqbal* operates as a “get out of jail free” card for defendants such as WSOD.

Plaintiff respectfully requests that this Court deny WSOD's Motion to Dismiss the Second Amended Complaint in its entirety, and move this case into class and merits discovery.

Dated: October 9, 2009

**s/Matthew R. Salzwedel**

Robert K. Shelquist (MN #021310X)  
Matthew R. Salzwedel (MN #0312903)  
Lockridge Grindal Nauen P.L.L.P.  
100 Washington Avenue South, Suite 2200  
Minneapolis, MN 55401  
Tel: (612) 339-6900  
Fax: (612) 339-0981  
rkshelquist@locklaw.com  
mrsalzwedel@locklaw.com

Myles McGuire, *admitted pro hac vice*  
Ryan D. Andrews  
KamberEdelson, LLC  
350 North LaSalle Street, Suite 1300  
Chicago, Illinois 60654  
Tel: (312) 589-6370  
Fax: (312) 589-6378  
mmcguire@kamberedelson.com  
randrews@kamberedelson.com

*Attorneys for Brenda Czech, individually, and on  
behalf of a class of similarly situated individuals*